REMARKS

The following remarks are made in response to the Office Action mailed June 1, 2010. Claims 7-9, 31, 33, and 34 have been previously cancelled. Claims 1-6, 10-16, 25-30, 32, 35-40, and 49-58 were rejected. Claims 17-24 and 41-48 have been objected to. With this Response, claims 25, 49, and 50 have been amended. Claims 1-6, 10-30, 32, and 35-58 remain pending in the application and are presented for reconsideration and allowance.

Claim Rejections under 35 U.S.C. § 101

The Examiner rejected claim 50 under 35 U.S.C. § 101 because the claimed invention is directed to non-statutory subject matter.

Claim 50 has been amended to be directed to statutory subject matter. Accordingly, Applicants submit that the above rejection of claim 50 under 35 U.S.C. § 101 should be withdrawn. Allowance of claim 50 is respectfully requested.

Claim Rejections under 35 U.S.C. § 102

The Examiner rejected claims 1-6, 10, 12, 25-30, 32, 36, and 49-58 under 35 U.S.C. § 102(e) as being anticipated by Winget, U.S. Patent Application Publication No. 2005/0086481 ("Winget").

Applicants submit the Winget fails to teach or suggest the features recited by independent claim 1 including "**providing, by an adjacent node, a component value B1 as a challenge to the first node; performing, by the first node, a handshake process with the adjacent node to determine membership in a secure group; wherein the handshake process comprises requiring each of the first node and the adjacent node to calculate identical values by applying the component values A1 and B1, and a key value associated with the secure group, to a one way function f(x).**"

Winget discloses a system and method for transmitting multicast messages via a wireless network (e.g., IEEE 802.11). (Para. [0006]). The system contemplates that trust relationships and the generation of keys may be established utilizing any known encryption scheme. (Para. [0034]). Following authentication and the development of a trust relationship between the components on the wired network, the access point (AP) may commence the

transmission of group ciphers. The AP is configured to transmit encrypted multicast exchanges to selected wireless clients. (Para. [0039]). The AP is configured to establish a group key name for each group cipher using a secure means, for example, a hash function. A hash function such as GTK[i]=SHA1-128 ("AP's Group KeyID"‖BSSID‖VLAN-ID‖128 bit-random-nonce) may be used to establish a unique group key name. Any desired hash function may be used to establish a group key name. The group key name need not be a function or derivation from the group key itself. The group key may be any uniquely identifiable value. (Para. [0041]).

Winget further discloses that once the group key name is embedded into a packet name extension, the data packets may then be transmitted by the AP to the wireless clients. The unique key name enables the wireless clients the ability to distinguish if the recipient is an intended addressee of the multicast transmission. (Para. [0044]). To determine if a wireless client is a member of the intended targeted group for the multicast transmission, the wireless client compares the validated group key name to elements contained within a local data table. (Para. [0048]). If the key name in the data table matches the received group key name, the message is deemed correctly delivered thereby prompting decryption of the entire message packet. If no key name in the local data table matches the received group key name, the message is discarded prior to any decryption attempt. (Para. [0049]).

The Examiner submits that the BSSID and the nonce of Winget disclose the *component value A1* provided by a *first node* and the *component value B1* provided by an *adjacent node*, respectively, as recited by claim 1. (Office Action, page 3). Winget does not disclose that a wireless client (i.e., an adjacent node) provides a nonce or challenge to the AP (i.e., the first node). In contrast, Winget merely discloses that the AP establishes a group key name for each group cipher using a hash function that includes the BSSID and a 128 bit-random-nonce (i.e., a random number used once). The random number or nonce is not provided by a wireless client. The wireless clients are not at all involved in the establishment of the group key names. Winget does not disclose a wireless client providing a challenge to the AP.

In addition, the Examiner cites paragraph [0041] of Winget as teaching *wherein the handshake process comprises requiring each of the first node and the adjacent node to*

calculate identical values by applying the component values A1 and B1, and a key value associated with the secure group, to a one way function f(x). (Office Action, page 4). Winget discloses that the AP establishes a group key name for each group cipher. (Para. [0041]). The wireless client does not calculate group key names, let alone calculate an identical group key name as the AP by applying the component values A1 and B1, and a key value associated with the secure group. The wireless client merely receives data packets including the group key name from the AP. The wireless client can then use the group key name to determine whether the recipient is an intended addressee of the multicast transmission. (Para. [0044]).

Winget does not disclose a handshake process where both the AP and the wireless client calculate identical values by applying a first component value provided by the AP, a second component value provided by the wireless client, and a key value associated with both the AP and the wireless client to a one way function f(x). In contrast, Winget appears to disclose that any handshake process is performed prior to the AP establishing the group key names. Winget discloses that the invention contemplates that trust relationships and the generation of keys may be established utilizing any known encryption scheme. (Para. [0034]). Winget further discloses that the methodology infers the pre-establishment of a trusted relationship between all components of the system (e.g. wireless clients, AP, switch, AS). (Para. [0057]). Winget fails to specifically disclose how the trusted relationship is established between all the components of the system prior to the AP's establishment of the group key names.

In view of the above, Applicants submit that the above rejection of independent claim 1 under 35 U.S.C. § 102(e) should be withdrawn. Dependent claims 2-6, 10, 12, 51, and 52 further define patentably distinct independent claim 1. Accordingly, Applicants believe that these dependent claims are also allowable over the cited reference. Allowance of claims 1-6, 10, 12, 51, and 52 is respectfully requested.

For similar reasons as discussed above with reference to independent claim 1, Applicants submit the Winget also fails to teach or suggest the features recited by independent claim 25 including "**wherein the handshake process comprises requiring each of the node and the adjacent node to calculate identical values by applying a**

component value A1 provided by the node, a component value B1 provided by the adjacent node, and a key value associated with the secure group, to a one way function f(x);" and the features recited by independent claims 49 and 50 including "**wherein each of the first node and the adjacent node has an identifier value that is associated with the secure group in order for the first node and the adjacent node to calculate identical values by applying a component value A1 provided by the first node, a component value B1 provided by the adjacent node, and the key value associated with the secure group, to a one way function f(x).**"

In view of the above, Applicants submit that the above rejection of independent claims 25, 49, and 50 under 35 U.S.C. § 102(e) should be withdrawn. Dependent claims 26-30, 32, 36, and 53-58 further define patentably distinct independent claim 25, 49, or 50. Accordingly, Applicants believe that these dependent claims are also allowable over the cited reference. Allowance of claims 25-30, 32, 36, 49, 50, and 53-58 is respectfully requested.

Claim Rejections under 35 U.S.C. § 103

The Examiner rejected claims 11, 13, 16, 35, 37, and 40 under 35 U.S.C. § 103(a) as being unpatentable over Winget in view of Traversat et al., U.S. Patent Application Publication No. 2002/0152299 ("Traversat").

Dependent claims 11, 13, 16, 35, 37, and 40 further define patentably distinct independent claim 1 or 25. Accordingly, Applicants believe that these dependent claims are also allowable over the cited references. Allowance of claims 11, 13, 16, 35, 37, and 40 is respectfully requested.

The Examiner rejected claims 14, 15, 38, and 39 under 35 U.S.C. § 103(a) as being unpatentable over Winget in view of Traversat and further in view of Mowers et al., U.S. Patent No. 7,644,275 ("Mowers").

Dependent claims 14, 15, 38, and 39 further define patentably distinct independent claim 1 or 25. Accordingly, Applicants believe that these dependent claims are also allowable over the cited references. Allowance of claims 14, 15, 38, and 39 is respectfully requested.

Allowable Subject Matter

The Examiner objected to claims 17-24 and 41-48 for being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all limitations of the base claim and any intervening claims.

Dependent claims 17-24 and 41-48 further define patentably distinct independent claim 1 or 25. Accordingly, Applicants believe that these dependent claims are also allowable over the cited references. Allowance of claims 17-24 and 41-48 is respectfully requested.

CONCLUSION

In view of the above, Applicants respectfully submit that pending claims 1-6, 10-30, 32, and 35-58 are in form for allowance and are not taught or suggested by the cited references. Therefore, reconsideration and withdrawal of the rejections and allowance of claims 1-6, 10-30, 32, and 35-58 is respectfully requested.

The Examiner is invited to contact the Applicants' representative at the below-listed telephone numbers to facilitate prosecution of this application.

Any inquiry regarding this Amendment and Response should be directed to Mark A. Peterson at Telephone No. (612) 573-0120, Facsimile No. (612) 573-2005.

Respectfully submitted,

Michael Roeder et al.

By their attorneys,

DICKE, BILLIG & CZAJA, PLLC
Fifth Street Towers, Suite 2250
100 South Fifth Street
Minneapolis, MN 55402
Telephone: (612) 573-2000
Facsimile: (612) 573-2005

Date: August 25, 2010
MAP:cjs

/Mark A. Peterson/
Mark A. Peterson
Reg. No. 50,485